UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/405,031	09/24/1999	DOUGLAS R. COFFLAND	IL-10360	9034

7590 02/20/2004

LLOYD E DAKIN JR
ASSISTANT LABORATORY COUNSEL
LAWRENCE LIVERMORE NATIONAL LABORATORY
P O BOX 808-L-703
LIVERMORE, CA 94551

EXAMINER	
BETIT, JACOB F	
ART UNIT	**PAPER NUMBER**
2175	6

DATE MAILED: 02/20/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/405,031	COFFLAND, DOUGLAS R.D	
	Examiner	Art Unit	
	Jacob F. Betit	2175	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6).MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *14 January 2004*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-30* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-30* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

DOV POPOVICI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Remarks

1. In response to communications filed on 14-January- 2004, claims 1, 10, 17, and 24 are amended per applicant's request. Claims 1-30 are presently pending in the application.

Claim Objections

2. Claims 10-16 are objected to because of the following informalities:

3. Claim 10 has two adjacent semicolons on line 5. The second semicolon needs to be removed.

Appropriate correction is required.

Claims 11-16 are objected to as being dependant on objected to independent claim 10.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 1-30 are rejected under 35 U.S.C. 103(a) as being unpatentable over Noll et al. (U.S. patent No. 5,732,138) in view of Owashi et al. (U.S. patent No. 6,363,210).

As to claim 1, Noll et al. teaches a system for multimedia encryption comprising:

a media signal (see column 4, lines 58-66), said media signal having the capacity of containing random noise that is completely unpredictable from one moment to the next or chaotic noise that is somewhat predictable over time (see column 4, lines 33-55);

a data module coupled to receive the media signal containing random noise that is completely unpredictable from one moment to the next or chaotic noise that is somewhat predictable over time (see figure 1, steps 100 and 105);

a data acquisition module coupled to receive and select a set of data (see figure 1, steps 100 and 105); and

a hashing module coupled to receive and hash the set of data into a keyword (see column 4, lines 20-23, where "keyword" is read on "seed").

Noll et al. does not teach multimedia encryption, and he does not teach a data compression module coupled to receive and compress the media signal into a compressed data stream and from the compressed data stream.

Owashi et al. teaches multimedia encryption (see column 1, lines 21-23), and he teaches a data compression module coupled to receive and compress the media signal into a compressed data stream and from the compressed data stream (see column 9, lines 6-10).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Noll et al. to include multimedia encryption, and a data compression module coupled to receive and compress the media signal into a compressed data stream and from the compressed data stream.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Noll et al. by the teachings of Owashi et al., because multimedia encryption would allow the multimedia provider charge money for access to the data stream (see Owashi et al., column 1, lines 21-23), and because a data compression module coupled to receive and compress the media signal into and from a compressed data stream would decrease the amount of data necessary for transmission (see Owashi et al., column 5, lines 59-62).

As to claim 2, Noll et al. as modified, teaches wherein the set of data is one frame of data within the compressed data stream (see Noll et al., column 4, lines 61-62).

As to claim 3, Noll et al. as modified, teaches wherein the set of data crosses over several frame boundaries within the compressed data stream (see Noll et al., column 4, lines 60-61).

As to claim 7, Noll et al. as modified, teaches wherein the media signal includes a noise signal amplitude (see Noll et al., column 4, lines 60-62, where "noise signal amplitude" is part of all transmitted signals);

further comprising,

an analog to digital converter (see Noll et al., column 2, line 3), having a quantization step size smaller than the noise signal amplitude coupled to receive and quantize the media signal (see Noll et al., column 1, line 67 through column 2, line 1, where it is assumed that in order to convert the noise from the diode into a signal not only does the frequency of the sample have to be suitable, but also "a quantization step size smaller than the noise signal amplitude" must exist); and wherein the data compression module compresses the quantized media signal into a compressed data stream (see Owashi et al., column 9, lines 5-10).

As to claim 8, Noll et al. as modified, teaches wherein the data compression module compresses the media signal into one from a group consisting of: MJPEG, MPEG1, MPEG2, or MPEG4, H.261, H.320, and H.323 formats (see Owashi et al., column 9, lines 5-13, see column 5, lines 59-62, and see column 14, lines 29-31).

As to claim 9, Noll et al. as modified, teaches further comprising:

a pseudo-random number generator coupled to receive and process the keyword in to a set of keywords (see Noll et al., column 4, lines 23-26).

As to claim 10, Noll et al. teaches a method (see Abstract) comprising the steps of:

a media signal having the capacity of containing random noise that is completely unpredictable from one moment to the next or chaotic noise that is somewhat predictable over time (see column 4, lines 33-55);

selecting a set of data (see figure 1, steps 100 and 105); and

hashing the set of data into a keyword (see column 4, lines 20-23 where "keyword" is read on "seed").

Noll et al. does not teach multimedia encryption; he does not teach compressing a media signal; and he does not teach set of data from the compressed media signal.

Owashi et al. teaches multimedia encryption (see column 1, lines 21-23); he teaches compressing a media signal (see column 9, lines 6-10); and he teaches set of data from the compressed media signal (see column 9, lines 6-10).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Noll et al. to include multimedia encryption; compressing a media signal; and set of data from the compressed media signal.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Noll et al. by the teachings of Owashi et al., because multimedia encryption would allow the multimedia provider to charge money for access to the data stream (Owashi et al., column 1, lines 21-23); because compressing a media signal would decrease the amount of data necessary for

transmission (see Owashi et al., column 5, lines 59-62); and because set of data from the compressed media signal would be an easy place to pull random data from to generate a random number.

As to claim 17, Noll et al. teaches a system, comprising:

a media signal having the capacity of containing random noise that is completely unpredictable from one moment to the next or chaotic noise that is somewhat predictable over time(see column 4, lines 33-55);

means for selecting a set of data (see figure 1, steps 100 and 105); and

means for hashing the set of data into a keyword (see column 4, lines 20-23, where "keyword" reads on "seed").

Noll et al. does not teach multimedia encryption; he does not teach means for compressing a media signal; and he does not teach set of data from the compressed media signal.

Owashi et al. teaches multimedia encyption (see column 1, lines 21-23; he teaches means for compressing a media signal (see column 9, lines 6-10); and he teaches set of data from the compressed media signal (see column 9, lines 6-10).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Noll et al. to include multimedia encryption; means for compressing media signal; and set of data from the compressed media signal.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Noll et al. by the teachings of Owashi et al., because multimedia encryption would allow the multimedia provider to charge money for access to the data stream (see Owashi et al., column 1, lines 21-23); because means for compression media signal would decrease the size of the data stream that needs to be transmitted (see Owashi et al., column 5, lines 59-62); and because set of data from the compressed media signal would be an easy place to pull random data from to generate the random number.

As to claim 24, Noll et al. teaches a computer-useable medium embodying computer program code (see column 6, lines 36-50) by executing the steps of:

a media signal having the capacity of containing random noise that is completely unpredictable from one moment to the next or chaotic noise that is somewhat predictable over time (see column 4, lines 33-55);

selecting a set of data (see figure 1, steps 100 and 105); and

hashing the set of data into a keyword (see column 4, lines 20-23, where "keyword" is read on "seed").

Noll et al. does not teach multimedia encryption; he does not teach compressing a media signal; and he does not teach set of data from the compressed media signal.

Owashi et al. teaches multimedia encryption (see column 1, lines 21-23); he teaches compressing a media signal (see column 9, lines 6-10); and he teaches set of data from the compressed media signal (see column 9, lines 610).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Noll et al. to include multimedia encryption; to include compressing a media signal; and to include set of data from the compressed media signal.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Noll et al. by the teachings of Owashi et al. because multimedia encryption would allow the multimedia provider to charge money for access to the data stream (see Owashi et al., column 1, lines 21-23); because compressing a media signal would decrease the amount of data necessary for transmission (see Owashi et al., column 5, lines 59-62); and because set of data from the compressed media signal would be an easy place to pull random data from to generate a random number.

As to claims 4, 13, 20, and 27, Noll et al. as modified, teaches wherein the compressed data stream includes compression transform coefficients (see Owashi et al., column 9, lines 6-10, where "compression transform coefficients" are a part of MPEG compression); and the set of data (see Noll et al., column 4, lines 60-61) includes a set of compression transform coefficients (see Owashi et al., column 9, lines 6-10).

As to claims 5, 14, 21, and 28, Noll et al. as modified, teaches wherein: the compressed data stream includes data frames of varying length (see Owashi et al.,

column 9, lines 9-13, where "frames of varying length" are made when compressing to MPEG format); and the set of data includes a set of data frames (see Noll et al., column 4, lines 60-61, and see lines 64-66).

As to claims 6, 15, 22, and 29, Noll et al. as modified, teaches wherein:

the compressed data stream includes predictive data frames (see Noll et al., column 2, lines 7-8); and the set of data includes a predictive data frame (see Noll et al., column 2, lines 7-8, see column 4, lines 60-62, and see figure 1, steps 100 and 105).

As to claims 11, 18, and 25, Noll et al. as modified, teaches wherein:

the compressed media signal includes data frames (see Owashi et al., column 9, lines 5-10); and

the selecting step includes the step of selecting one frame of data (see Noll et al., column 4, lines 61-62).

As to claims 12, 19, and 26, Noll et al. as modified, teaches wherein:

the compressed media signal includes data frames and data frame boundaries (see Owashi et al., column 9, lines 5-13, where "data frames" are recognized to vary in size in MPEG format); and

the selecting step includes the step of selecting a set of data which crosses over several data frame boundaries (see Noll et al., column 4, lines 61 -62).

As to claims 16, 23, and 30, Noll et al. as modified, teaches wherein the media signal includes a noise signal amplitude (see Noll et al., column 4, lines 60-62, where "noise signal amplitude" is part of all signals);

further comprising the step of quantizing the media signal with a quantization step size smaller than the noise signal amplitude (see Noll et al., column 1, line 67 through column 2, line 1, where it is assumed that in order to convert the noise from the diode into a signal not only does the frequency of the sample have to be suitable, but also "a quantization step size smaller than the noise signal amplitude" must exist); and

wherein the compressing step includes the step of compressing the quantized media signal (see Owashi et al., column 9, lines 5-10).

Response to Arguments

6. Applicant's arguments filed on 14-January-2004 have been fully considered but they are not found persuasive:

In response to the applicant's arguments that "the Owashi et al. Reference does not disclose a system for multimedia encryption having the capacity of containing random noise that is completely unpredictable from one moment to the next or chaotic noise that is somewhat predictable over time or a data compression module coupled to receive and compress the media signal containing random noise that is completely unpredictable from one moment to the next or chaotic noise that is somewhat predictable over time into a compressed data stream", the arguments have been fully

considered but are not deemed persuasive because the primary reference, Noll et al., teaches the media signal containing random noise that is completely unpredictable from one moment to the next or chaotic noise that is somewhat predictable over time. The secondary reference, Owashi et al., teaches "a data compression module coupled to receive and compress the media signal" as shown in the remarks and discussions made above.

In response to the applicants arguments that "the Noll et al. Reference is limited to a chaotic source", the arguments have been fully considered but are not deemed persuasive because the claims offer a choice between a completely unpredictable noise and a chaotic noise. As long as the Noll et al. reference teaches one of these, it satisfies the requirements of a 35 USC 103 (a) rejection.

In response to the applicant's arguments that "neither the Noll et al. Reference or the Owashi et al. Reference show Applicant's claim elements 'media signal having the capacity of containing random noise that is completely unpredictable from one moment to the next' or 'a data compression module coupled to receive and compress the media signal containing random noise that is completely unpredictable from one moment to the next,'" the arguments have been fully considered but are not deemed persuasive because the Applicant's claims offer a choice between "media signal having the capacity of containing random noise that is completely unpredictable from one moment to the next" and "chaotic noise that is somewhat predictable over time" and a choice

between "a data compression module coupled to receive and compress the media signal containing random noise that is completely unpredictable from one moment to the next" and "chaotic noise that is somewhat predictable over time". Noll et al. as modified, teaches "chaotic noise that is somewhat predictable over time" and "chaotic noise that is somewhat predictable over time into a compressed data stream" (see Noll et al., column 4, lines 33-55), which satisfies the requirement of the claims.

In response to applicant's arguments that "there is no suggestion or motivation to combine the Noll et al. Reference and the Owashi et al. Reference to produce Applicant's invention", the arguments have been fully considered but are not found persuasive because the examiner recognizes that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988) and *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992). In this case, the examiner is establishing motivation in the knowledge generally known to one of ordinary skill in the art. Both cited references teach inventions that are in the same field of endeavor. The primary reference, Noll et al. teaches a method for producing a chaotic binary string from a media input that is then hashed and used as a seed in a pseudo-random number generator. The pseudo-random numbers can then be used as cryptographic keys (see abstract), which is very much in line with the teachings of the present invention. The

secondary reference, Owashi et al. teaches a system for communication encryption (abstract) in which he teaches multimedia encryption (see column 1, lines 21-23); a data compression module coupled to receive and compress the media signal into a compressed data stream (see column 9, lines 6-10); and set of data from the compressed media signal (see column 9, lines 6-10). Therefore, a person having ordinary skill in the art at the time the invention was made would be motivated to modify the invention of Noll et al. by the teaching of Owashi et al. because multimedia encryption would allow a multimedia provider to charge money for access to the data stream (Owashi et al., column 1, lines 21-23), because compressing the media signal would decrease the amount of data necessary for transmission (see Owashi et al., column 5, lines 59-62), and because a set of data from the compressed media signal would provide an easy already available place to pull data from to generate a random number for the multimedia encryption. It is well known in the art, as can be seen from the Noll et al. patent, that a multimedia signal can be used to generate a random number, and as can be seen by the Owashi et al. patent, that a random number is needed to encrypt a video signal and that data compression is used to decrease the amount of data necessary for transmission.

In response to applicant's arguments that "the teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in prior art, and not based on applicant's disclosure", it must be recognized that any judgment on obviousness is in a sense necessarily a reconstruction based upon

hindsight reasoning. But so long as it takes into account only knowledge which was within the level of ordinary skill at the time the claimed invention was made, and does not include knowledge gleaned only from the applicant's disclosure, such a reconstruction is proper. See *In re McLaughlin*, 443 F.2d 1392, 170 USPQ 209 (CCPA 1971).

Conclusion

7. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

8. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jacob F. Betit whose telephone number is (703) 305-3735. The examiner can normally be reached on Monday through Friday 9 am to 5 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Dov Popovici can be reached on (703) 305-3830. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

jfb
February 9, 2004

DOV POPOVICI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100